Strategy Research Project

PROVIDING AN ENTERPRISE SERVICE ARCHITECTURE TO THE NET-CENTRIC WARFIGHTER

BY

LIEUTENANT COLONEL DAVID P. ACEVEDO
United States Army

USAWC CLASS OF 2008

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2008	**Strategy Research Project**	**00-00-2007 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Providing an Enterprise Service Architecture to the Net-Centric Warfighter	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
David Acevedo	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**32**	

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

USAWC STRATEGY RESEARCH PROJECT

PROVIDING AN ENTERPRISE SERVICE ARCHITECTURE TO THE NET-CENTRIC WARFIGHTER

by

Lieutenant Colonel David P. Acevedo
United States Army

Lieutenant Colonel Charles Grindle
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel David P. Acevedo

TITLE: Providing an Enterprise Service Architecture to the Net-Centric Warfighter

FORMAT: Strategy Research Project

DATE: 10 March 2008 WORD COUNT: 5,521 PAGES: 32

KEY TERMS: Communications, Network, Transformation, Joint Warfighting, Network Centric Warfare

CLASSIFICATION: Unclassified

To meet the challenges of the future, the Department of Defense (DoD) must have a strategy to ensure the joint forces of tomorrow will be able to achieve full spectrum dominance through the use of networks and access to enterprise data services that provide true interoperability, seamless integration and available on demand collaboration. Joint procedures for the implementation of deployed collaboration capabilities on DOD networks within local enclaves or domain wide must be synchronized to achieve the greatest efficiencies at home station and when deployed. The objective is to provide a capability for the near-term implementation of an Active Directory (AD) environment capable of support in Generating Force (GF) environments while maintaining the ability to seamlessly deploy and integrate into Deployed Force (DF) architectures. A Joint directory and enterprise service strategy provides the potential for significantly enhanced interoperability, seamless integration and collaboration capabilities through which these objectives can be achieved. This paper will examine existing AD deployment policies and guidance and how a joint strategy

using the concept of Theater Resource Forest (TRF) architecture will greatly enhance interoperability and collaboration across the force.

PROVIDING AN ENTERPRISE SERVICE ARCHITECTURE TO THE NET-CENTRIC WARFIGHTER

> At the end of the day, our warfighters really only want one thing— rapid and reliable access to the network, their data and applications from stable and unchanging computer configurations as they move from home station, through mission rehearsals, and into theater operations.[1]
>
> —Commander NETCOM, MG Carroll F. Pollett,

Evolving operational needs and the ability to share information across functional, organizational and unit boundaries remains problematic as identified in seven of the nine combatant commands Integrated Priority Lists (IPLs).[2] Recent experiences in Iraq and Afghanistan demonstrate the need for better cross organizational information sharing strategies that will guide the transition from today's information sharing paradigm to a net-centric paradigm.[3] The limitation in access to required information, collaboration and knowledge sharing capabilities is impacting commanders' abilities to gain true situational awareness in today's Volatile, Uncertain, Complex and Ambiguous (VUCA) operational environments.

Future combat forces are expected to rapidly deploy into a theater of operations capable of operating in joint and multinational environments and able to coordinate operations with other U.S. Government and selected civil organizations.[4] The ability to fight immediately upon arrival requiring little or no systems reconfiguration places increased demands on how the military designs and operates its networks. Theater operations will continue to be joint and multinational, resulting in the need for greater levels of cooperation and integration between U.S. forces, other DOD components, coalition and host-nation organizations.[5] As military missions grow more complex,

robust communications and network integration and interoperability will become increasingly vital to warfighting operations.

The Department of Defense (DOD) accelerated its transformation efforts following the terrorist attacks of September 11, 2001. These sweeping transformation efforts increased integration, interoperability, and focus on net-centricity greatly accelerating the transformation of Joint, Interagency, and Multinational (JIM) warfighting capabilities as never experienced before.[6] As a result, today's joint force is more expeditionary, modular and agile.[7] The reality of this transformation, as well as operational requirements, demands that information be increasingly shared within and across organizational boundaries while at home station and when deployed.[8] Tactical and maneuver elements rely on networks to leverage strategic and national capabilities which allow them to deploy and fight upon arrival.[9] This creates a complex environment that demands commanders have full network connectivity and integration through an Enterprise Service Architecture (ESA) that provides access to the network immediately and to fight.[10] To achieve full integration and interoperability requires the continued expansion of the "joint team mindset" from the combatant command (COCOM) level down to the JTF and component headquarters.[11] The elimination of seams between functional components and within the DOD will enhance this integration creating the ability to truly share information across time and space.

The intent of this SRP is to examine current policy and guidance on the implementation of Active Directory (AD) and to recommend a strategy that facilitates better integration of these architectures to provide enterprise level services. This analysis does not provide the technical procedures required for installing, operating or

maintaining AD but instead provides a conceptual framework for providing shared access to enterprise level resources. Contained within this paper will be an examination of the current Army AD policy as it relates to units in home station, their relationship with the Local and Area Processing Centers (LPC's/APC's), and the transition of tactical units away from home station into deployed operations. I will address a strategy for the development of a Resource Forest [12] (RF) architecture that will work in coexistence with the current Army and Joint Task Force-Global Network Operations (JTF-GNO) AD architecture policies and guidance. I will establish how the RF strategy provides enhanced integration that strikes the right balance between control, security, autonomy and flexibility while keeping the fundamental principle of "work and train as we fight." I will further demonstrate how separate Generating Force (GF) and Deployed Force (DF) Forest leveraging a common Enterprise Application Resource Forest (EARF) will provide for a consistent and acceptable secure means to host enterprise level services and share them across a joint force providing net-centricity through a Service Oriented Architecture (SOA). Through this analysis, I will illustrate how the implementation of the EARF concept will minimize the need for systems reconfiguration and administrative coordination during the transition process as tactical units deploy in support of DF operations. The EARF concept minimizes security risk and allows for the greatest level of transparency, flexibility and integration for deploying units while ensuring continuity of operations and access to critical information and collaboration resources throughout all phases of operations. In the conclusion, I will summarize my analysis and answer the question of what supporting AD architecture can be applied that provides for increased information, collaboration and knowledge sharing capabilities.

Primer on Active Directory

Directory and Enterprise Services are key elements to the military and DOD networks providing the essential foundation to the theater network support infrastructure for access and collaboration.[13] All successful operating systems today work off of a core Directory Service (DS) that controls access to resources. At the component and enclave level, the primary DS supporting the joint forces and DOD is Microsoft's Active Directory product.[14] Active Directory is Microsoft's implementation of an international DS standard. In the DOD environment, AD forms the nucleus for all activities. This spans authentication, permissioning, digital identity, online "presence", the presentation of a Global Address List (GAL) through Exchange and state management. Active Directory provides for integration, increased interoperability and supports the Net Centric Enterprise Service (NCES) architecture for the DOD and other governmental agencies. Active Directory also allows for the distribution, management and oversight of globally deployed Group Policies Objects (GPO) providing flexibility in maintaining the health of the network and enterprise services through the application of Information Assurance (IA), antivirus definitions and installation of new applications; all managed and deployed from a central point across the enterprise.[15]

In short, AD is the DS for many DOD components and essential to the net-centric vision. In order to be net-centric, any infrastructure needs to provide a consistent identity, access, and policy enforcement foundation. Active Directory provides this foundation for access to Enterprise Services (ES) and is generally the accepted DS across the LandWarNet,[16] the DOD and the Global Information Grid (GIG).[17]

Active Directory in the Modular Force

The United States Army created modular units that are self-contained, sustainable and organized with capabilities for the full range of missions that provide for better integration and interoperability to support the joint environment.[18] Presently, Corps, Divisions and Brigades are all granted permission to operate and maintain their own NIPR[19] and SIPR[20] AD Forest while in both the GF and DF environments.[21] These multiforest [22] structures do not inherently allow for the separation of domain enclaves of user accounts, exchange and enterprise application services outside of the same Forest structures. These multiforest structures are implemented independently and cannot easily share resources with each other.

The most significant advantage of the modular force is greater strategic, operational, and tactical flexibility.[23] Although this flexibility ensures the most effective support to the warfighter, it presents significant challenges to achieving and maintaining transparency, integration and security when designing and implementing the supporting AD infrastructures. As stated by Vice Adm. Nancy E. Brown, USN, previous C6 for the Multi-National Forces – Iraq (MNF-I) and now the Director for Command, Control, Communications and Computer (C4) Systems (J-6), the Joint Staff, Washington, "Active Directory was supposed to be a panacea. Well, the way we've implemented it, it's no different than what we've ever had before. We implemented Active Directory just like we've done everything else: We've done it by service, and there's no interdependence at all; in fact, there's little interoperability if you look at it."[24]

The Army's AD multiple Forest approach provides for separate Forests that can operate autonomously, for theaters of operation, brigades, and higher tactical deployable units.[25] This multiforest approach allows for units to exercise full operational

control for all assigned AD Forests and equipment at the expense of providing a secure shared Area of Responsibility (AOR) based resource environment.[26] Modular Bde's data networks are intended to be interconnected with the ability to operate autonomously during the early phases of an operation then interdependently when able to connect in a theater capable of providing enterprise level support and services. The transformation towards systems of interdependence while maintaining the capability of modular units to operate independently will increasingly require data architectures that provide access to enterprise applications and services in the deployed environment and at home station. It is this necessity for autonomy and interdependence, while maintaining operational and tactical control that must remain consistent as the DOD moves forward with its NCES concept and provides for the seamless transition of tactical units from GF environments, away from home station into combat theaters of operations. As the 16th Chairmen the Joint Chiefs of Staff states when addressing the capabilities of joint warfighting and transformation: "Joint warfighting …it is a prerequisite to winning the War on Terrorism and will significantly accelerate and be accelerated by transformation. This will require collaborative and innovative solutions to difficult cultural and resource challenges. The future joint forces must transition from an interoperable to an interdependent force where different capability sets can be rapidly integrated to achieve desired effects."[27]

Using the CONOPS for Implementing AD in Tactical Army Units, autonomous units are defined as "any unit that satisfies the Joint Expeditionary Mindset (Task Force Modularity) and can be deployed without regard to any habitual relationship or Task Organization CONUS or otherwise."[28] Within these units (Corps, Div, and BCT's)

consists a single AD Forest structure and a single AD domain.[29] As a result, and in order to share information across Forest and domain boundaries, requires the establishment of a "meshed" architecture that makes it difficult to define the authoritative sources of information and requires an inordinate amount of administration and coordination overhead (see trust) to gain coherence in information and knowledge sharing. Using this meshed architecture by establishing "trust relationships" during the pre-deployment and deployment phases, requires the Enterprise Administrators for each Forest to coordinate with all other units that are part of the deployment to set the deployment architecture and establish a series of "transit trust" between each.[30] This is necessary to ensure the sharing of information and is in compliance with DOD Directive Number 8320.02 dated December 2, 2004; that states "Data assets shall be made accessible by making data available in shared spaces. All data assets shall be accessible to all users in the Department of Defense except where limited by law, policy, or security classification. Data that is accessible to all users in the Department of Defense shall conform to DOD-specified data publication methods that are consistent with GIG enterprise and user technologies."[31]

As described, in order for tactical Army units, sister services and governmental organizations to share information seamlessly across Forest boundaries requires a series of trust relationships to be established. However, trusts may only be established between DF Forests that are task organized (headquarters and sub-elements assigned, attached, or OPCON) for deployment or training. Trusts between DF Forests that are not task organized are not permitted.[32] This prevents the establishment of a net-centric and enterprise service architecture required to share information throughout the force.

Using the RF concept, the data architecture for a theater of operations consolidates enterprise level services at the JTF, theater or regional level, greatly reducing the number of required AD trust relationships. This will enable future forces to move from interoperable and autonomous operations to a more interdependent force where capabilities and the desired effects are achieved through the integration of systems across the force.[33]

Challenges and Observations OIF 05-07

During Operation Iraqi Freedom (OIF) 05-07, within the Iraq AOR, there existed no less than 27 separate Army tactical AD Forest (there are more than 200 in the tactical Army AD structure)[34] and more than 40 in the CENTCOM AOR presenting significant challenges to integration, transparency and security. The ability to access and share information across Div, Bde and Corps Forest boundaries was limited. Seamless access to other governmental agencies and to sister services was even more problematic requiring intense administrative coordination and account duplication resulting in users need for multiple accounts and logons. The Corps installed, operated, and maintained three separate data networks NIPR, SIPR and CENTRIXS[35] for e-mail, collaboration, Voice Over Internet Protocol (VoIP), video-teleconferencing, SharePoint and Command Post of the Future (CPoF). Lack of unity in a joint AD structure created problems in every security domain. This made it difficult to replicate Global Address List (GAL), drive consistency in the application of security related group policies, centralize configuration and manage from an enterprise level. This was further complicated by limited bandwidth to the Modular Brigades located in Forward Operating Bases (FOB's) and in some cases only limited knowledge of operating enterprise Information

Technology (IT) services to include Microsoft AD.[36] As a result, the AD architecture creates a "disjointed" information sharing environment causing commanders to stovepipe information impacting the ability to synchronization efforts to achieve the desired effects. A unified AD structure will lead to better synchronization, enable net-centricity, ease system administration, and allow for access to information and collaboration while increasing mobility for the warfighter.

Introduction to the Resource Forest (RF)

The basis for my RF discussion is predicated upon the understanding of the following: 1) The DOD Network Centric Enterprise Services (NCES) is not yet fully implemented. 2) The establishment of the Local and Area Processing Centers is not yet completed. 3) The Army will continue transformation requiring self supporting modular units. 4) The GIG is not fully mature to support tactical units reach back for access to enterprise level services.[37] 5) Forward deployed tactical units will continue to operate within their own AD Forest structures at home station and when deployed. 6) The continued requirement to interoperate in a joint environment with our sister services and the equipment they bring to the fight.

A large strategic theater network ensures continuity of information to incoming organizations and enables units to "fall in" on an operational IT infrastructure – achieving mission readiness on the first day in country through rapid integration.[38] The need for immediate access to resources and the ability to collaborate across the force is a fundamental war fighting requirement. Supporting tactical systems are expected to seamlessly integrate becoming interdependent as a Theaters Information Grid (TIG) matures. Tactical units must be able to deploy from home station into any theater of

operations with limited or no systems reconfiguration or disruption of service. This essential requirement represents an expected level of service and data interoperability between tactical units. The Army's multiforest approach is the best AD topology supporting the modular force and the integration of the GF into DF operations. The multiforest approach allows large organizations, such as the Army and DOD, that have multiple modular units and supporting organizations to deploy separate AD structures as it provides for the greatest level of autonomy and security.[39] The RF topology is a supporting multiforest configuration that is used for hosting application services and is supported as part of the CONUS GF AD architecture.[40]

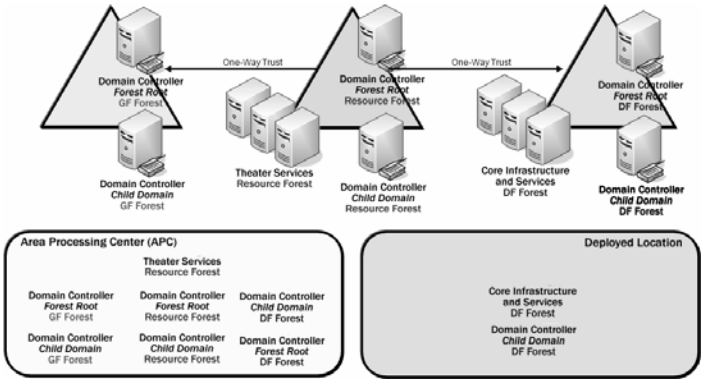

Figure 1.

The concept of an EARF is not complex. Simply put, it is a separate Forest that hosts enterprise level applications that are available to all organizations either deployed or in a supporting GF environment. Users who need access to these enterprise applications authenticate through their own AD Forest structures and gain access to resources and services that reside within the RF. It is this architecture that allows for a common "hosting" of services at the enterprise level that can be shared and accessed

across the force while ensuring the proper standardization, security and configuration management in support of the net-centric architecture.

The RF Forest is a “hub and spoke” architecture that provides for a “non meshed” infrastructure that greatly reduces the administration (at the tactical level) and coordination overhead required when sharing information across multiple Forest boundaries. The EARF concept allows tactical units to leverage strategic resources while maintaining mobility on the battlefield which enhances information sharing. The same is true when autonomous units are at home station; access to resources is shared by both the GF and DF user base by establishing a separate Forest to host enterprise level services that can be accessed by both. For example, this is particularly useful for a Corps Headquarters under transformation that supports a Main Command Post (MCP), an Operational Command Post and the Early Entry Command Post (EECP). Under this structure, much of the planning and support is provided from the MCP at home station and forward to the OCP and EECP. As a result, all CP’s can now access a common enterprise structure hosting a set of services that is separate and distinct from the Forest structure supporting the MCP for garrison operations. This greatly reduces the security risk of extending the garrison Forest structure into a combat theater of operations by placing essential enterprise services into separate Forest that can be extended or deployed with an OCP/EECP.

The Theater Network Architecture

Although much progress has been made, interoperability remains an illusive goal that the U.S. military and the DOD continues to fight on many fronts.[41] As observed by the Multi-National Corps – Iraq Commander in 2005: “In Iraq, battle command spanned

the full spectrum of joint and coalition warfighting concerns, to include policy differences on how we protect our data networks through information assurance, service differences on networking and collaboration, the standards necessary to implement active directories, and our ability to share information in a complex architecture."[42]

The network-centric force is structured around concepts of Knowledge Management that requires access to information and people whenever and wherever they are. This requires an extensive, standardized, interoperable and well protected enterprise service architecture that provides continuity of information, ease of access, and the ability to provide the right services to the right location at the right time. The theater network architecture applies "jointness" to systems engineering, design, planning, deployment, and operation of enterprise information services.[43] As joint forces are increasingly networked, linked and synchronized; dispersed forces are able to better communicate, share information and collaborate.[44] NETCOM's long term objective end state to achieve this is to provide the tactical portion of the Army Enterprise Infostructure (AEI) by extending the network and access to enterprise services (NCES) from Army component commanders in a GF environment to deployed forces supporting a joint, combined, or single-service task force conducting expeditionary operations.[45] Until this vision can be realized, DF forces must be able to access key resources resident in a theater of operations while maintaining their modular flexibility to deploy and integrate into theater network centric architectures.

NETCOM established that while Brigade Combat Teams (BCTs) are at home station, they will leverage LPC/APC enterprise services through the installations networks via the establishment of Virtual Local Area Networks (VLANS) and through the

Joint Network Nodes (JNN) when training using the Regional Hub Nodes.[46] Deployed forces will access enterprise level applications and resources via reach-back through Standardized Tactical Entry Point facilities (STEP) [47] or Teleport sites to an APC location.[48] It is this architecture that allows for the centralized management of services that must be incorporated into DF architectures that are deployed forward and available immediately upon arrival into theaters of operations. As stated by the CENTCOM J6 when addressing a panel on JTF interoperability, "Operational information, data, knowledge sharing requirements exceeds the ability of the existing infrastructure. Data management strategies and Tactics, Techniques and Procedures (TTPs) are needed to disseminate and stage information *forward* in support of the Warfighter at the *first* tactical mile."[49] As stated, information must be staged forward; to accomplish this, the best approached is one designed and supported by applying the principles of an Enterprise Service Architecture forward in the fight.

Trust in a Multiple Forest Approach

The Army's AD multiple Forest approach decentralizes the operations and maintenance of its directory services to tactical units.[50] This provides for the greatest level of autonomous operations while presenting significant challenges to administrators and the ability to share information and collaborate across AD Forest boundaries. To allow users in one domain to access resources in another, AD uses Forest and trusts.[51] The Forest concept is intended to simplify both end-user access to the directory and management of multiple domains. Utilizing the multiple Forest approach, all domains and trees[52] in a Forest inherently trust one another for the purpose of authentication. Such trusts are not extended automatically between Forests, which requires directory

administrators in modular units to manually configure trusts between Forests.[53] This is necessary as Microsoft defines the security boundary for AD Forest enclaves to reside at the Forest level.[54] This is also necessary as the availability of enterprise applications and collaboration services such as SharePoint, databases and applications specific to Communities of Interest (COI) require tactical units to authenticate users across Forest boundaries. As a result, for tactical units to authenticate users within their own Forest structures and gain access to resources in other tactical Forest requires coordination and "trust" relationships between participating organizations. This is problematic as trusts may only be established between DF Forests that are task organized (headquarters and sub-elements assigned, attached, or OPCON). Trusts between DF Forests that are not task organized are not permitted thereby limiting access to shared resources.[55]

Presently, the Army alone supports more than 200 tactical Forests within its tactical AD architecture.[56] In a theater of operations such as Iraq, and in order to share information and collaborate with every other Forest owner, requires the establishment of multiple separate AD trust relationships each requiring written approval by the DAA.[57] Without these trust relationships, units cannot easily share information and collaborate across their Forest boundaries. Although trust relationships in themselves are not problematic, the management of these relationships requires intensive administrative oversight and directly impacts the ability to maintain transparency and seamless integration into a Theaters Information Grid (TIG) immediately upon arrival. As an AOR is typically transitional in nature, units are constantly rotating in and out of theater

requiring them to reestablish trust relationships with other rotating units to ensure total access.

Security in a Multiforest Architecture

The necessity to establish AD trust relationships between Forest owners requires a level of security that is agreed upon throughout the DOD.[58] The AD Security Technical Implementation Guide (STIG) provides security and standardization configuration guidance for the implementation of Active Directory within the Department of Defense. The STIG is designed to assist System Administrators (SAs), Information Assurance Managers (IAMs), Security Managers (SMs), and Information Assurance Officers (IAOs), with the implementation of AD configurations and is intended to provide a certain level of security compliance assurance.[59] It also allows for individual sites to determine the level of assurance that is appropriate to their environment and mission.[60] Experience demonstrates that organizations do not always adhere to the security guidance established by their component service or within the DOD. As a result, this creates a level of "mistrust" between Forest owners and prevents the establishment of a cohesive and robust information sharing environment. To alleviate this mistrust, units must be required to validate their AD environments during their Mission Rehearsal Exercises (MRE's) in accordance with the policies and guidance provided by the DOD and their supporting COCOM. As previously mentioned, validation of all AD structures will ensure the ability of deploying units to seamlessly integrate into a combat theater of operations and ensure the required access to key resources and applications.

An Examination in the Successful Implementation of a RF

The ability to dynamically collaborate and share information requires an architecture that provides services that are immediate available and easily accessible to units in transition and within a theater of operations. The deployment of the RF in Iraq is an example of an ESA that provides theater level services supporting forces in a highly mobile environment.[61] In the Iraq Theater of Operations (ITO), to establish information sharing between modular unit Forest and the theater Forest requires one of the following: 1) Establish individual accounts on the hosting theater account domain. 2) Establish trust relationships between users supporting Forest account domains and the theater Forest domains. It is important to note the establishment of this trust only allows for the sharing of information between these two Forests. The following are advantages and disadvantages of RF architecture model.

Advantages	**Disadvantages**
• Provides for enterprise data sources that can be managed centrally or through a shared administration model. Provides Net-Centricity	• Creates an additional Forest at the enterprise level
• Reduces the need to migrate information to incoming and outgoing units thereby easing access to information	• Requires enterprise administration oversight
• Supports modularity while reducing the administrative burden	• Requires organization to change their culture to share information
• Can be grown into a regional or theater resource capability	• Requires additional infrastructure
• Provides for better integration and access to information across organizational boundaries	• Added complexity to develop the initial design
	• Requires corporate "buy in" for this non traditional approach

Table 1.

Multiple Accounts on Multiple Domains

Without AD trust relationships between unit domains structures, individual accounts must be created in the hosting account domain. This creates the need for multiple accounts and log-ons across multiple security domains. This presents a significant security challenge as external users can not be positively identified and abuse of user accounts and passwords becomes evident (Figure 2).

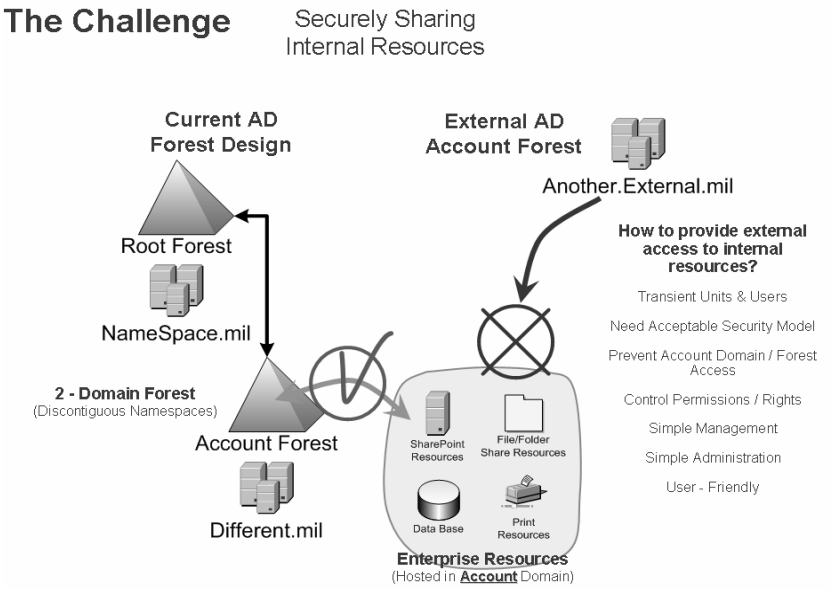

Figure 2.[62]

To eliminate this vulnerability using the RF architecture, users are authenticated through their own supporting account domains inherent in their modular AD Forest structures.[63] This provides the mechanism whereby an organization hosting enterprise level services can accept that external users have already been authenticated by a trusted partner and can grant them access; without having to be responsible for managing their identity information. Within this framework, users enjoy seamless, secure access to enterprise services and multiple applications. This not only simplifies

the process of granting access, it also makes it possible to maintain the high levels of security necessary to protect the integrity of that access.

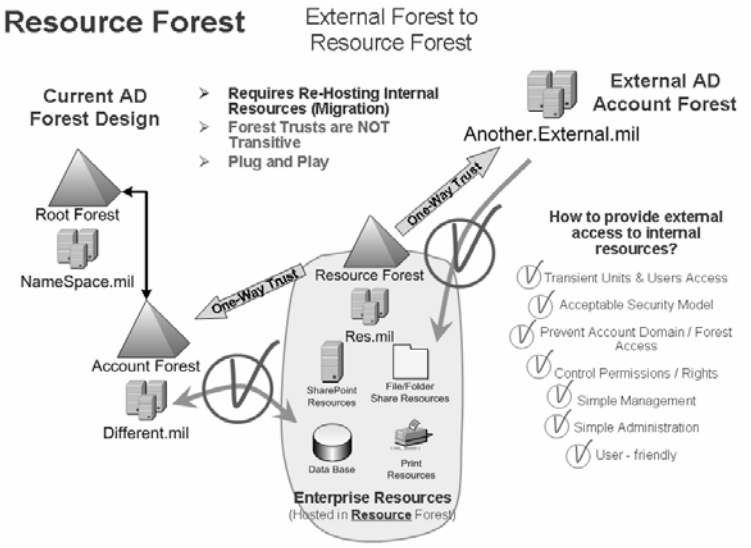

Figure 3. [64]

Providing Resource Access

The correct method of providing access to shared resources is to create domain local groups in the RF and assign access rights and permissions to those groups.[65] Then access to resources within the RF is easily managed by adding domain global groups (or individual user accounts) from external domain(s) to the domain local groups in the RF. Since this method uses domain local groups in the RF, those groups are restricted to the RF. In other words, domain local groups can not be used external to the RF so it is not possible to transfer them or their members outside of the RF structure.[66] This method of providing external access to hosted services is under the complete control of the hosted service's administrative account(s) within the RF. In other words, administrators for a hosted service are fully enabled to manage access and security for their services and resources. This architecture provides for the greatest

level of unit control for unit applications with no assistance needed from RF Administrators.

Flexibility

The RF Forest topology provides for the greatest level of flexibility and allows for the ability to rapidly affect change in the operational environment. As previously described, the current tactical implementation guidance for AD requires Forest owners to establish trust relationships with every other Forest owner. This limits the organizations flexibility as they are often re-task organized or have a change in mission requiring trust relationships to be broken then re-established under the new task organization. A single trust relationship to an EARF limits the amount of coordination and administrative overhead while greatly increasing the continuity of operations and information sharing capabilities, regardless of task organization. The RF architecture also provides flexibility by using the shared administration model between enterprise administrators and the resource owners. Under this concept, resources are hosted within the RF structure and maintained by the owning organization. It provides for premier support as the DF can leverage expert resources when hosted within the LPC/APC or at the highest levels within a DF theater architecture. Because the RF is a shared administrative model, users can host services within the RF domain structure maintaining unit control and access.

Transparency

Transparency allows for the access to the resources a war fighter needs to accomplish his/her mission while deployed or in garrison. Currently, forces cannot quickly deploy IT services as large amounts of resources are spent creating and

disabling accounts for end users that move from one geographical location to another or from GF to DF environments.[67] Tactical Forces are not able to move about an AOR quickly gaining access to systems, enterprise applications or a common GAL as Forest level trust between units remains fractured.[68] Without an enterprise level architecture for access to key resources, units are forced to operate within their own information domains with limited or no access to theater level information or collaboration services. In the RF architecture, all hosted services can be managed individually and permissions to resources provided by the hosted services can be managed by group memberships or individual user accounts from any trusted external domain. Units gain increased mobility by accessing a single enterprise resource Forest where all information can be shared and collaborated between multiple Forest owners. This approach greatly reduces the number of required trust between Forest owners and minimizes the administrative and coordination requirements.

Standardization

For AD to interoperate efficiently, the DOD must adhere to a set of standards that are enforced across the GIG. Active Directory inherently requires that trust relationships be established to share information and collaborate between Forest and domains. Adherence to standards as determined by the DOD will minimize the problems associated with “mistrust” between Forest owners. However, adhering to standards in not enough; tactical AD structures must be exercised and evaluated during the pre-deployment stages of operations to ensure their ability to integrate into the TIG upon arrival.

People and Organizations, Changing the Culture

The greatest challenge to gaining net-centricity is changing the cultures of the organizations in which we operate. As we move from an interoperable force to a more interdependent force, organizations are increasingly challenged to share information within and across organizational boundaries. To achieve this requires organizations to adopt the joint team mindset and willingness to share information openly. Forces must design their supporting AD structures not by service but instead by standards set by the joint community at large. The DOD vision describes a future state where transparent, open, agile, timely, and relevant information sharing occurs that promotes freedom of maneuverability across a trusted information environment.[69] To achieve the vision requires organizations that encourage, and incentivize sharing; achieves an extended and available enterprise; strengthens agility in order to accommodate unanticipated partners and events; and ensures trust across organizations.[70]

Final Recommendations

It is clear that AD policies and strategies must increasingly address the need to shared and collaborate across organizational boundaries to include those agencies within the Department of State the DOD and other governmental organizations. The development of a SOA founded on the principles of transparency, interoperability, and work as we fight while maintaining the flexibility necessary to operating in today's complex environments is required. Until the Army's WIN-T and NCES programs can fully be realized, tactical units require an architecture that allows for the seamless deployment from home station and into a combat theater of operations with the ability to quickly gain access to key resources and applications. One conceptual way to

accomplish this, and how the Army is currently doing this in Iraq, is to establish a separate RF for the hosting of key services and applications. This concept consists of multiple AD Forest with a shared Forest /domain managed at the regional or theater level. This concept provides for faster deployment as it decreases organizational complexity, maintains unit autonomy while providing for interdependence, decreases the number of log-ons required by people who reside outside in their own tactical Forest structures and maintains an acceptable level of security risk.

In order to provide an Enterprise Service Architecture to the warfighter in today's net-centric environment, the following recommendations are made.

1) Place key enterprise services and applications in separate AD Forests at the JTF, Theater or regional level.
2) Develop a SOA that limits the number of AD trust relationships required to support the sharing of Information.
3) Enforce and validate standards that promote interoperability and information exchange for all deploying units and organizations.
4) Maintain a culture of jointness and information sharing by designing and implementing data architectures that are joint focused.

Conclusion

The disjointed Forest structure that has emerged out of programmatic decisions, and the lack of trust, leads to an architecture that does not promote or establish the open sharing of information and collaboration across the DOD. The DOD and the Army must establish a data architecture that allows users spanning multiple domains to efficiently and reliably manage information and gain access to key resources. Access to

common enterprise level resources and services is significantly improved using the EARF model.

The DOD NCES will be essential to implementing a network-based information environment that provides for increased information sharing and collaboration thereby enabling decision superiority. It will offer the core enterprise services based on Communities of Interest that will provide for common access to centrally hosted resources accessible through the GIG. Until this vision can be realized, DF and supporting organizations must have access to resources and services that are shared across organizational boundaries at home station and where deployed.

The concept of a RF is slowly gaining ground and is being explored by NETCOM as a solution to better enable the warfighter. Recently, NETCOM hosted an "RF Summit" to determine the validity of the concept. It was determined that although additional technical details still need to be developed, the concept of the RF will "eventually solve many of the problems associated with access to resources in environments supporting multiple Forest."[71]

Endnotes

[1] Military Information Technology Online, LandWarNet Transformer: *Strengthening Operational Responsiveness and Security*, available from http://www.military-information-technology.com/article.cfm?DocID=2142; Internet; accessed 23 November 2007.

[2] VADM Nancy Brown, Director, C4 Systems, Joint Staff J6, Command Control, Communications and Computer Systems Directorate, "Joint Net-Centric Operations Campaign Plan," available from http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf; Internet; accessed 5 January 2008.

[3] Ibid.

[4] U.S. Joint Forces Command, "Standard Operating Procedure & Tactics, Techniques, and Procedures, For the Standing Joint Force Headquarters Core Element," 14 December 2004, 4.

[5] U.S. Department of the Army, *Signal Support to Theater Operations*, Field Manual Interim 6-02-45, (Washington, D.C.: U.S. Department of the Army), available from http://www.fas.org/irp/DODdir/army/fmi6-02-45.pdf; Internet; accessed 23 November 2007.

[6] Brown.

[7] Ibid.

[8] U.S. Army Chief Information Office, *The Army Knowledge Management, Strategic Plan*, 2d ed. (Washington, D.C.: U.S. Government Printing Office, 2003), 1-4.

[9] U.S. Department of the Army, *Joint Operations*, Joint Publication 3.0 (Washington, D.C.: U.S. Department of the Army), available from http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf; Internet; accessed 2 February 2008.

[10] U.S. Department of the Army, *Signal Support to Theater Operations*, Field Manual Interim 6-02-45 (Washington, D.C.: U.S. Department of the Army), available from http://www.fas.org/irp/DODdir/army/fmi6-02-45.pdf; Internet; accessed 20 November 2007.

[11] Joint Operations Concepts, “An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution In the 21st Century,” available from https://augateway.maxwell.af.mil/affor/text/evolve/joc.htm; Internet; accessed 15 January 2008.

[12] Microsoft overlays the generic domain structure with architecture described as “Forests and trees”, where the trees are individual domains and a Forest consists of a group of domains, who selectively share a common set of trusts and applications. Each Forest has an Active Directory service that lists all of the users and applications as well as who, according to the Access Control List, is allowed to connect to whom within the Forest.

[13] U.S. Department of Defense, *Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise* Version 1.0, available from http://www.defenselink.mil/ cio-nii/docs/GIGArchVision.pdf; Internet; accessed 17 January 2008.

[14] U.S. Department of Defense, *Active Directory Security Technical Implementation Guide*, Version 1, Rel 1, available from http://iase.disa.mil/stigs/stig/active-directory-stig-v1r1.pdf; Internet; accessed 19 January 2008.

[15] Ibid.

[16] LandWarNet is the Army's portion of the Global Information Grid (GIG) supporting users around the world. LandWarNet is the combination of infostructure and services across the Army. It provides for processing, storing, and transporting information over a seamless network. It is the Army counterpart to the Air Force ConstellationNet and the enterprise network of the Navy’s Force Net.

[17] For background on the Global Information Grid, see U.S. Department of Defense, Defense Information Systems Agency; GIG Bandwidth Expansion, available from http://www.disa.mil/ main/prodsol/gig_be.html; Internet; accessed 3 January 2008.

[18] U.S. Department of the Army, United States Army Signal Center, Directorate Of Combat Developments Concepts and Doctrine Division, *Concept for Implementation of Active Directory in Tactical Army Units*, Version 1.0 (Washington, D.C.: U.S. Department of the Army, 10 July 2006). iii.

[19] The "NIPRNET," the Unclassified but Sensitive Internet Protocol Router Network (formerly called the Non-secure Internet Protocol Router Net), is a network of Internet protocol routers owned by the Department of Defense (DOD). Created by the Defense Information Systems Agency (DISA), NIPRNET is used to exchange unclassified but sensitive information between "internal" users. It can thus be distinguished from the Secret Internet Protocol Router Network (SIPRNET), which is used by the DOD to exchange classified information in a totally secure environment.

[20] Ibid.

[21] Ibid., 1.

[22] For background on the Microsoft Forest and Active Directory Design, see Microsoft Technet, Microsoft Windows Server 2003 Active Directory, available from http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx; Internet; accessed 3 January 2008.

[23] U.S. Department of the Army, *Signal Support to Theater Operations*, Field Manual Interim 6-02-45 (Washington, D.C.: U.S. Department of the Army), available from http://www.fas.org/irp/DODdir/army/fmi6-02-45.pdf; Internet; accessed 20 November 2007.

[24] Maryann Lawlor, “Transforming through Jointness,” Signal, 61, 66-68, 70 (June 2007): [journal online]; available from ProQuest; accessed 6 February 2008.

[25] U.S. Department of the Army, U.S. Army Signal Center, Directorate of Combat Developments Concepts and Doctrine Division, *Concept for Implementation of Active Directory in Tactical Army Units*, Version 1.0 (Fort Gordon, 10 July 2006), iii.

[26] U.S. Department of the Army, U.S. Army Signal Center, Directorate of Combat Developments Concepts and Doctrine Division, Fort Gordon, Georgia, 30905-5735, *Concept for Implementation of Active Directory in Tactical Army Units*, iii.

[27] GEN Peter Pace, Chairman of the Joint Chiefs of Staff, *Shaping the Future* October 2005, available from http://integrator.hanscom.af.mil/2005/October/10132005/PaceGuidance02Oct05.pdf; Internet; accessed 6 January 2008.

[28] U.S. Department of the Army, U.S. Army Signal Center, Directorate of Combat Developments Concepts and Doctrine Division, Fort Gordon, Georgia, 30905-5735, *Concept for Implementation of Active Directory in Tactical Army Units*, A-1.

[29] Ibid.

[30] Ibid., 12.

[31] U.S. Department of Defense, *Data Sharing in a Net-Centric Department of Defense*, Directive 8320.02, available from http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf; Internet; accessed 27 December 2007.

[32] NETCOM/9TH Signal Command (Army) Technical Authority (TA), *Implementation Memorandum U.S. Army Enterprise Systems Technology Activity (ESTA)*, (Fort Huachuca, AZ.: U.S. Army, June 2006); Implementation Memorandum Number 2006-006, 9.

[33] Ibid.

[34] U.S. Department of the Army, U.S. Army Signal Center, Directorate of Combat Developments Concepts and Doctrine Division, Fort Gordon, Georgia, 30905-5735, *Concept for Implementation of Active Directory in Tactical Army Units*, 1-6.

[35] Combined Enterprise Regional Information Exchange System (CENTRIXS) is the premier network for coalition interoperability in support of military operations. Ongoing coalition operations continue to test and prove the viability of the CENTRIXS enterprise. Information flow to coalition partners via the multiple versions of CENTRIXS networks achieved unprecedented volume and continues to expand.

[36] U.S. Congressional Research Service Report for Congress, Network Centric Warfare: Background and Oversight Issues for Congress, 2 June 2004, available from http://www.fas.org/man/crs/RL32411.pdf; Internet; accessed 2 February 2008.

[37] BG Jeffery Smith stated in his Army Presentation at the recent Microsoft Conference that NSC is a 5 year pay off, and LTG Sorenson briefed it as part of the 10-15 POM for DA G6 in his keynote.

[38] U.S. Department of the Army, U.S. Army Signal Center, Directorate of Combat Developments Concepts and Doctrine Division, Fort Gordon, Georgia, 30905-5735, *Concept for Implementation of Active Directory in Tactical Army Units*, 1-6.

[39] Ibid.

[40] Ibid., 17.

[41] Lawlor.

[42] LTG John R. Vines, Commander XVIII Airborne Corps, *The XVIII ABC on the Ground in Iraq,* available from http://usacac.army.mil/CAC/milreview/English/SepOct06/Vines.pdf; Internet; accessed 27 December 2007.

[43] U.S. Department of the Army, Signal Support to Theater Operations, Field Manual Interim 6-02-45 (Washington, D.C.: U.S. Department of the Army), available from http://www.fas.org/irp/DODdir/army/fmi6-02-45.pdf; Internet; accessed 20 November 2007.

[44] Ibid., 1-2.

[45] Ibid.

[46] NETCOM/9TH Signal Command (Army) Technical Authority (TA).

[47] Sites that provide access to DISN via Defense Satellite Communications (DSCS) X-band terminals.

[48] NETCOM, Army NETOPS CONOPS, ver 1.0, available from https://ascp.monmouth. army.mil/ scp/downloads/standardspolicy_files/NETCOM_NETOPS_CONOPS_v10_1.pdf. 2-12.

[49] COL Chris Wilhelm, CCJ6 Information Brief to JTF Interoperability Panel (U), Chief, Communications Plans and Operations Division, USCENTCOM CCJ6-C, 9 May 2006.

[50] U.S. Department of the Army, U.S. Army Signal Center, Directorate of Combat Developments Concepts and Doctrine Division, Fort Gordon, Georgia, 30905-5735, *Concept for Implementation of Active Directory in Tactical Army Units*, 1.

[51] For background on the Microsoft Directory Structures, see Microsoft TechNet, Windows 2003 Resource Kit, available from http://www.microsoft.com/technet/prodtechnol/ windows2000serv/reskit/gloss/reskitgloss.mspx?mfr=true; Internet; accessed 3 January 2008.

[52] Ibid.

[53] John Fontana, "*Active Directory 'Forests' May Cause Pain*," *Network World*, 17, 16, 124. (February 2000): [journal online]; available from ProQuest; accessed 6 February 2008.

[54] U.S. Department of Defense, Active *Directory Security Technical Implementation Guide*, Version 1, Rel 1, available from http://iase.disa.mil/stigs/stig/active-directory-stig-v1r1.pdf; Internet; accessed 17 January 2008.

[55] NETCOM/9TH Signal Command

[56] U.S. Department of the Army, U.S. Army Signal Center, Directorate of Combat Developments Concepts and Doctrine Division, Fort Gordon, Georgia, 30905-5735, *Concept for Implementation of Active Directory in Tactical Army Units*, A-1-A-5.

[57] Ibid.

[58] For background on the Microsoft Directory Structures, see Microsoft TechNet, Windows 2003 Resource Kit, available from http://www.microsoft.com/technet/prodtechnol/ windows2000serv/reskit/gloss/reskitgloss.mspx?mfr=true; Internet; accessed 3 January 2008.

[59] U.S. Department of Defense, *Active Directory Security Technical Implementation Guide*, Version 1, Rel 1, available from http://iase.disa.mil/stigs/stig/active-directory-stig-v1r1.pdf; Internet; accessed 17 January 2008.

[60] Ibid.

[61] The discussion on the Resource Forest and concept of implementation in Iraq is credited to Automation Services Division for MNC-I during rotation 05-07 supported by the V Corps and the follow-on rotation 05-08 supported by the III Corps. This concept is not officially documented

but was approved by the MNC-I Information Services Division Chief during OIF 05-07 and further executed and documented by the MNC-I III Corps.

[62] CW2(P) Anthony Dennis, USA, Multi-National Corps Iraq, Information Services Division C6 Services Technician; 14 December 2007.

[63] Ibid.

[64] Ibid.

[65] CW2(P) Anthony Dennis and Mr Brent Gatewood, USA, Multi-National Corps Iraq. *The Resource Forest Cookbook*, interview by authors, 8 November 2007.

[66] Ibid.

[67] NETCOM, Army NETOPS CONOPS.

[68] Ibid.

[69] U.S. Department of Defense, Office of the Chief Information Officer, *Department of Defense Information Sharing Strategy*, available from http://www.defenselink.mil/cio-nii/docs/InfoSharingStrategy.pdf; Internet; accessed 15 January 2008.

[70] Ibid.

[71] CW3 Ross Ball, USA, Network Engineer Network Enterprise Technology Command/9th Signal Command Army, interview by author, 8 February 2008.